Proteggere i Dati Aziendali on-premises e nel cloud

Antonio Forzieri

Cyber Security Practice Lead, Global
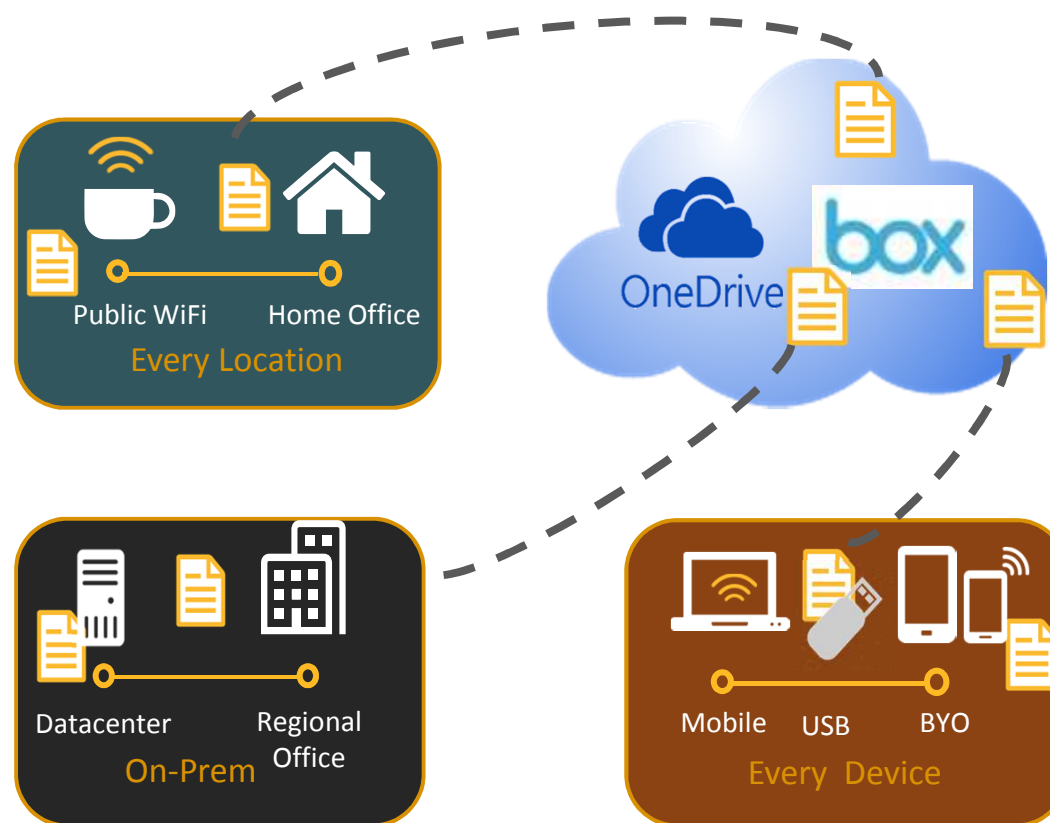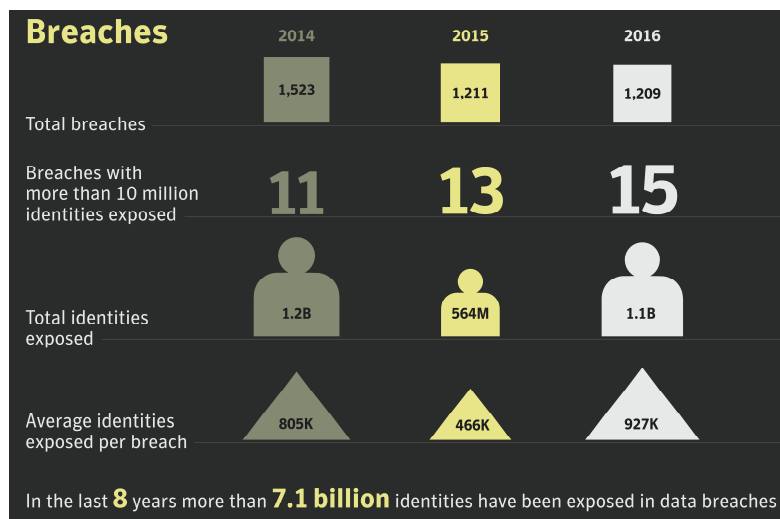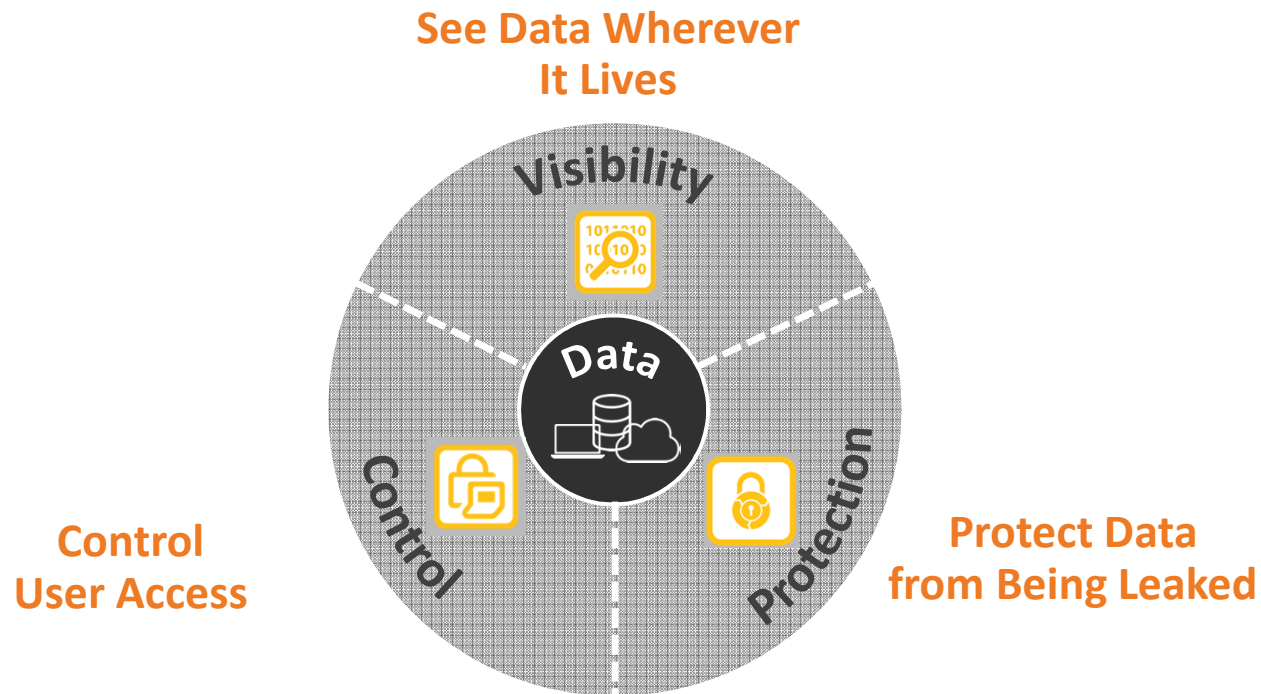
Agenda

Challenges with information protection in the cloud

Breaches	2014	2015	2016
Total breaches	1,523	1,211	1,209
Breaches with more than 10 million identities exposed	**11**	**13**	**15**
Total identities exposed	1.2B	564M	1.1B
Average identities exposed per breach	805K	466K	927K

In the last **8** years more than **7.1 billion** identities have been exposed in data breaches

Public WiFi   Home Office
Every Location

OneDrive   box

Datacenter   Regional Office
On-Prem

Mobile   USB   BYO
Every Device

Delivering Information Centric Security

See Data Wherever It Lives

Visibility

Data

Control

Protection

Control User Access

Protect Data from Being Leaked

Symantec Information Centric Security(ICS) Components

☑ **Data Loss Prevention (DLP)**

Discovers sensitive data across all channels with central policy controls

☑ **CloudSOC (CASB)**

Extends existing DLP policies, workflows, and detection to Cloud Apps

☑ **Validation and ID Protection Service (VIP)**

Secures access to critical data with Multi-Factor Authentication

☑ **NEW Information Centric Encryption (ICE)**

Integrated policy driven encryption and identity access
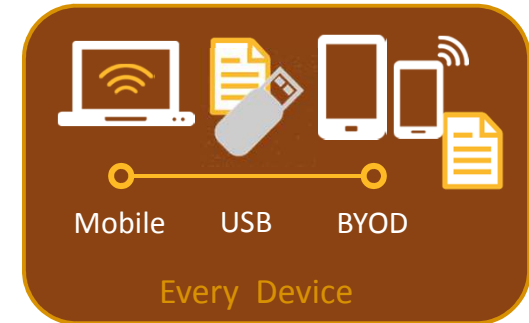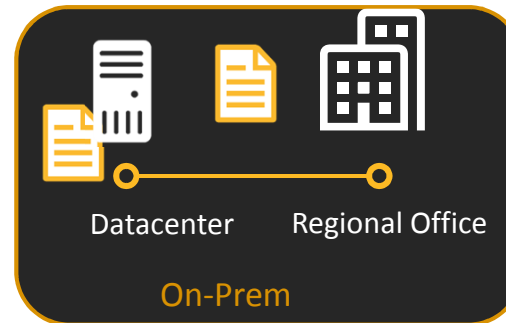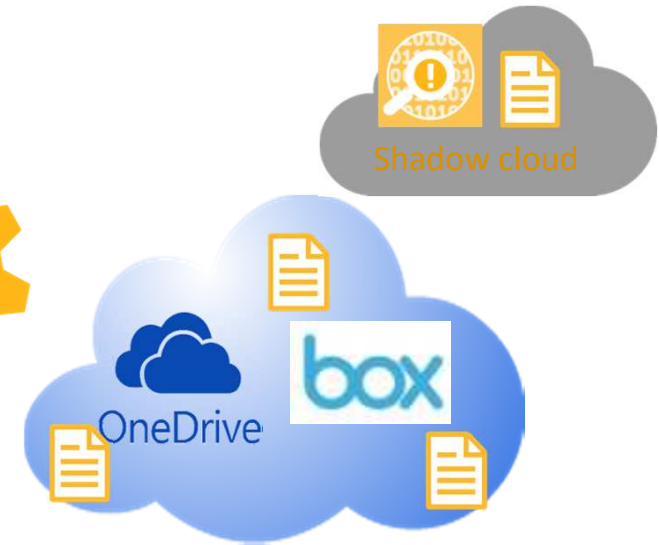
☑ **NEW Information Centric Tagging (ICT)**

Increases DLP efficiency with User driving DLP tagging

DLP · **CloudSOC** · **ICT** · **ICE** · **VIP**

Visibility · **Control** · **Protection** · **Data**
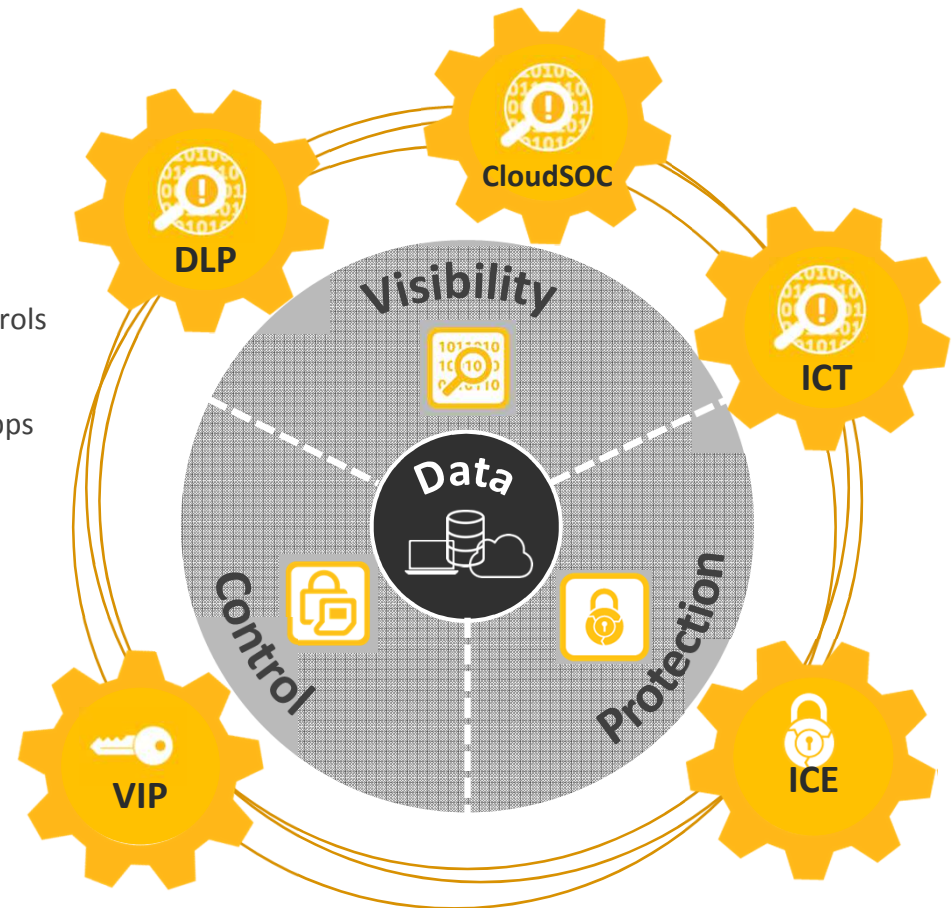
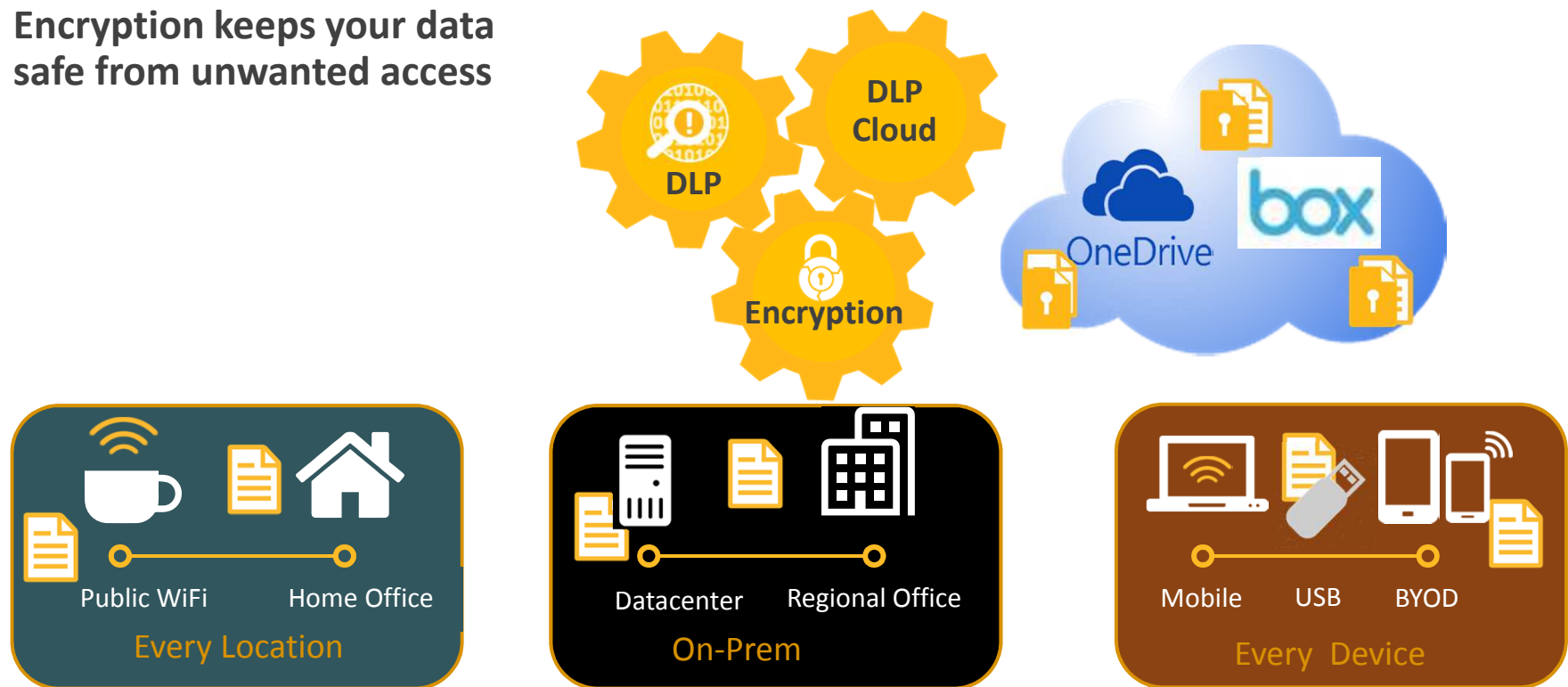# How do I get visibility of sensitive data?

DLP gives visibility of sensitive data across any channel.

DLP Cloud + CloudSOC gives visibility of Shadow IT in sanctioned and unsanctioned cloud apps.

Shadow cloud

DLP

DLP Cloud

OneDrive

box

Public WiFi   **Home Office**

Every Location

Datacenter   **Regional Office**

On-Prem

Mobile   **USB**   **BYOD**

Every Device

How do I protect my data when it is outside of my control?

Encryption keeps your data safe from unwanted access

DLP Cloud

DLP

Encryption

OneDrive

box

Every Location
- Public WiFi
- Home Office

On-Prem
- Datacenter
- Regional Office

Every Device
- Mobile
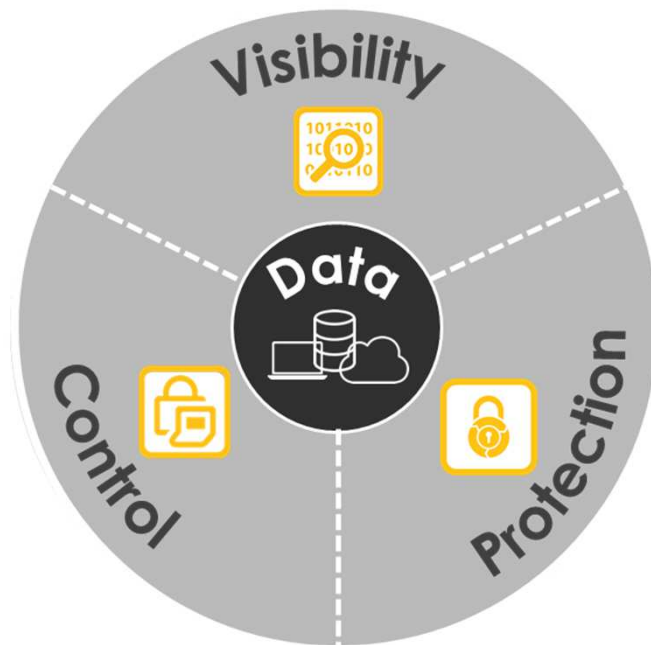- USB
- BYOD

How can I ensure my data will not be compromised?

Multi-Factor Authentication (MFA) controls access by protecting your data from stolen credentials

ICE supports other SAML v2.0 solutions

DLP

DLP Cloud

VIP

Encryption

OneDrive

box

Public WiFi   Home Office
Every Location

Datacenter   Regional Office
On-Prem

Mobile   USB   BYOD
Every Device
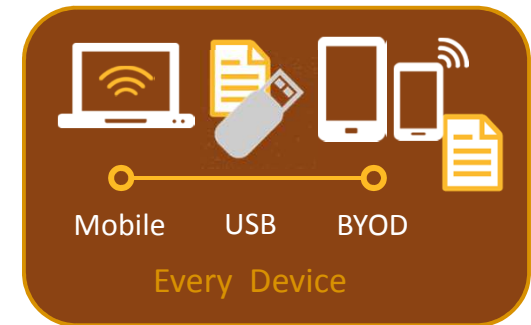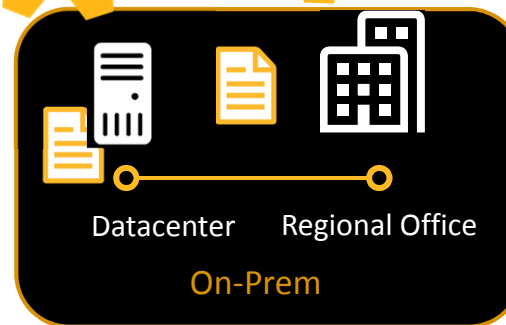
Allow the right people to access the right data by …

…monitoring its flow…

…protecting it
wherever it goes…

…controlling access
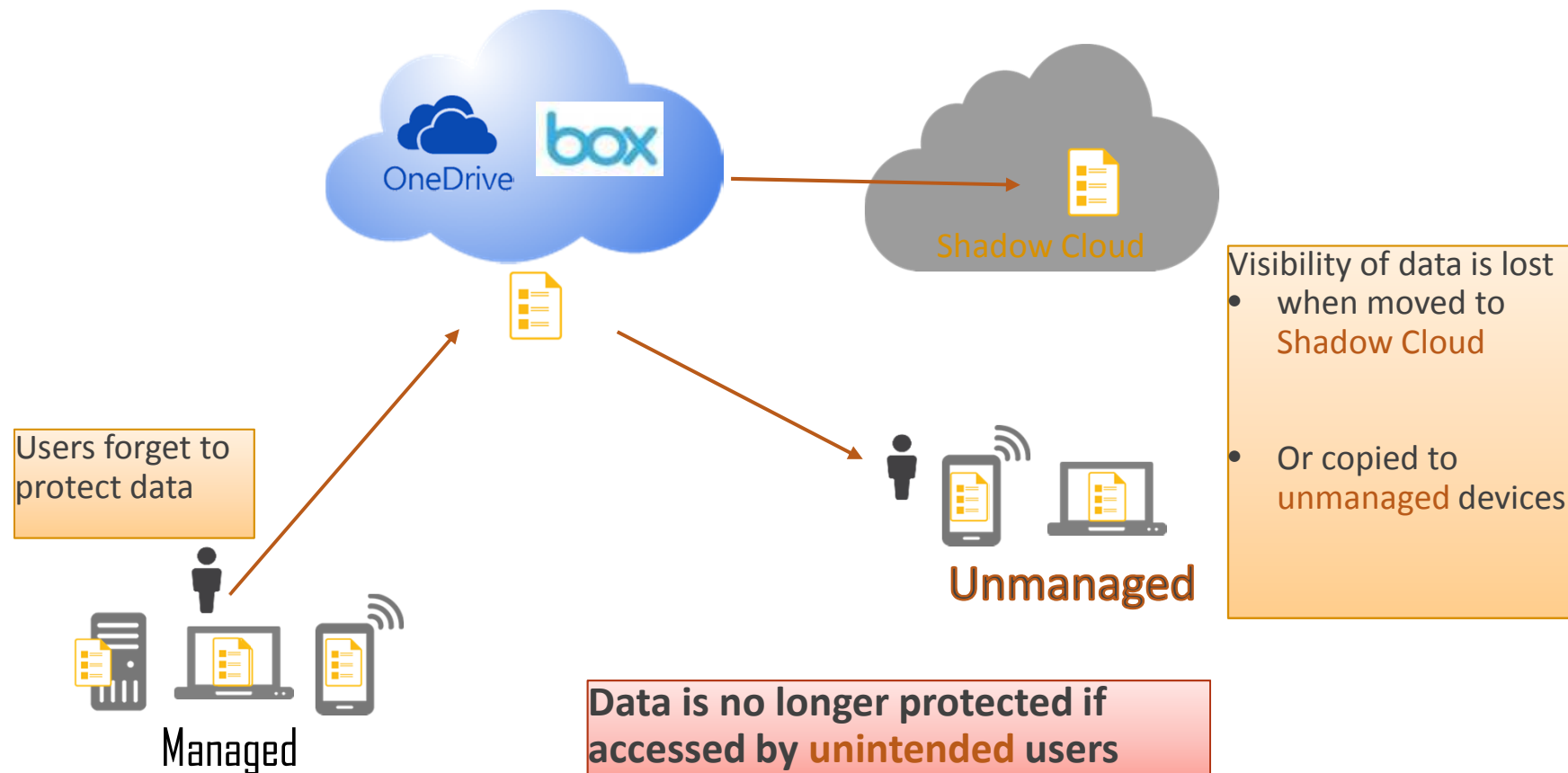and keeping it out of the
wrong hands

Symantec Information Centric Encryption
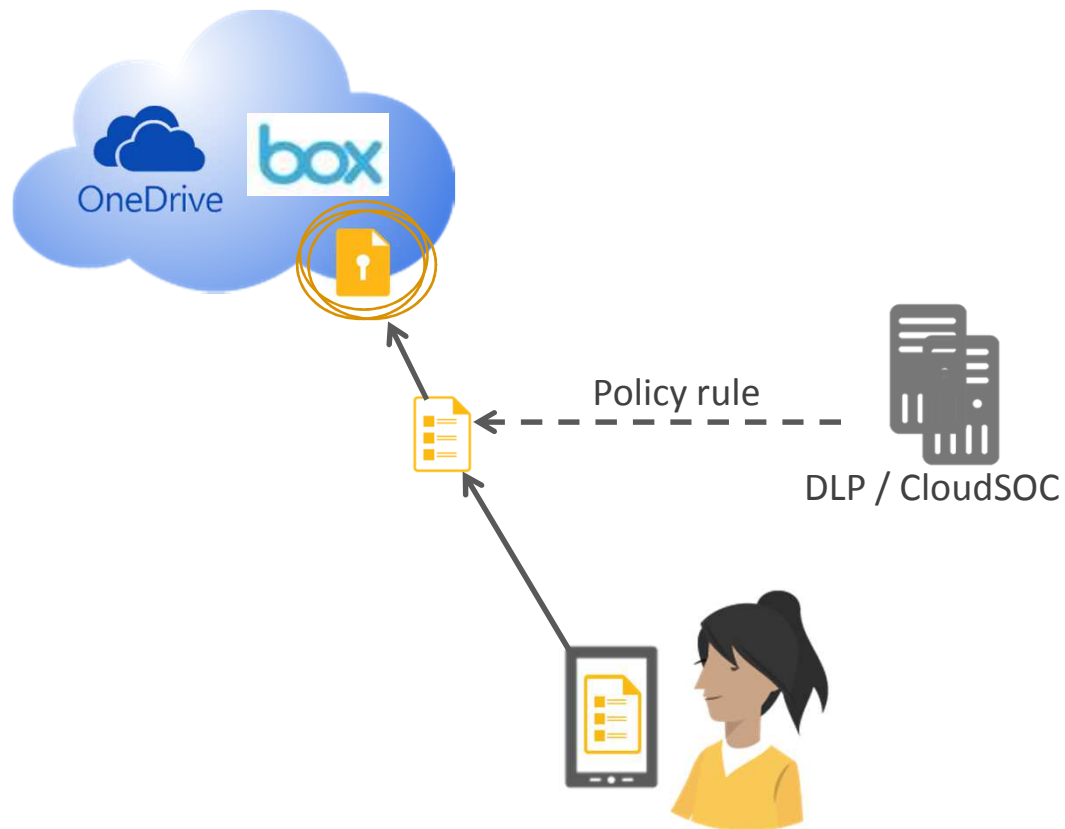
Addressing Business Objectives

Challenge: I need to protect data on premise, in the cloud, and on mobile

Visibility of data is lost
- when moved to Shadow Cloud

- Or copied to unmanaged devices

Users forget to protect data

Unmanaged

Managed

Data is no longer protected if accessed by unintended users

Solution: Enforce encryption before data is moved out of the organisation
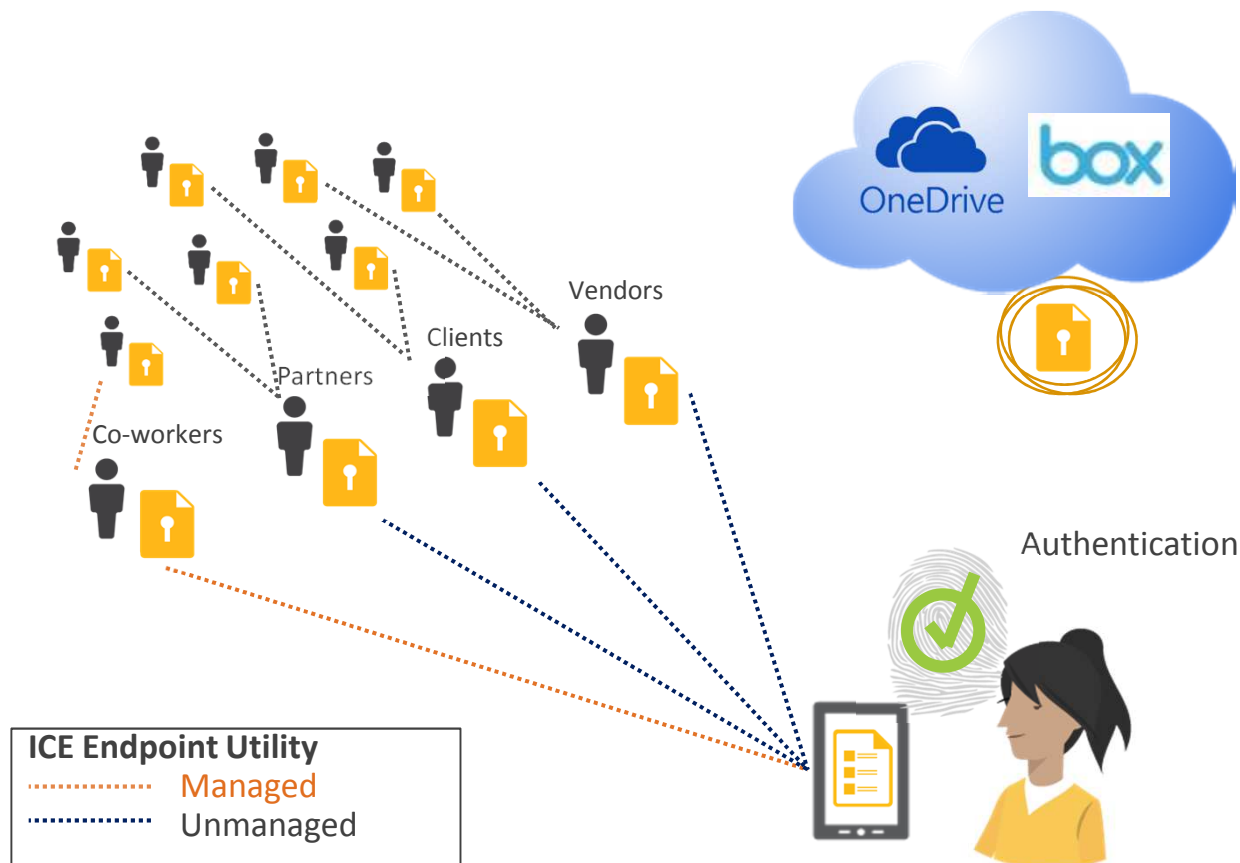
Policy rule

DLP / CloudSOC

1. CloudSOC intercepts file

2. Automated DLP policies ensure file is protected

3. ICE encrypts the data and creates a protective wrapper around the data

Challenge: Sharing data in the cloud can be risky and inefficient
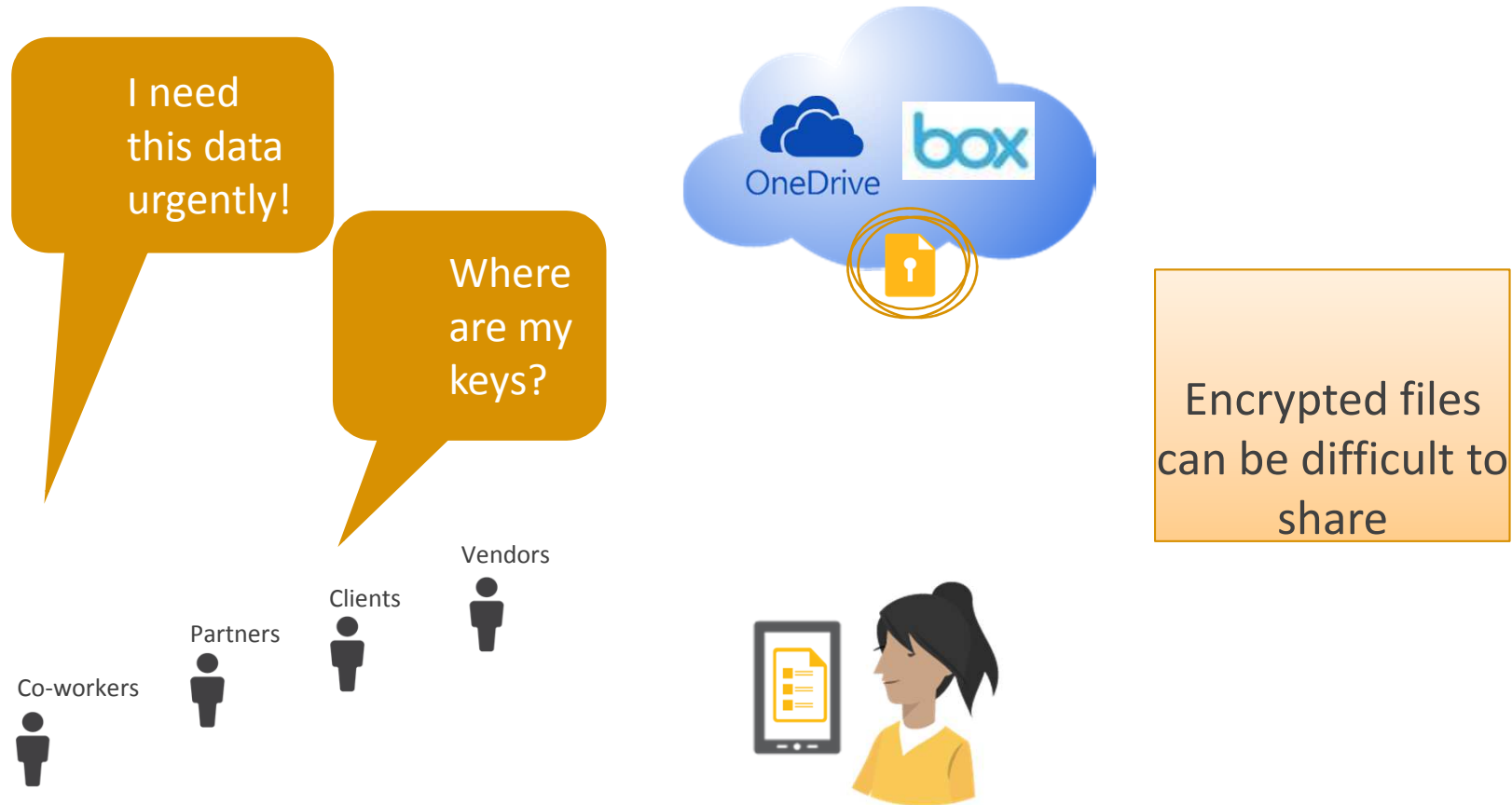
Solution: Manages encryption and keys for easy data sharing

Vendors

Clients

Partners

Co-workers

OneDrive

box

Authentication

ICE Endpoint Utility
.... Managed
.... Unmanaged

- ICE identity services ensures efficient authentication

- CloudSOC encrypts using ICE libraries

- Windows and Mac ICE Endpoint Utility supported

- Unmanaged users need to download utility and register

14

Challenge: How can I remain in control of my data and prove it?

How can I recall all copies?

How do I know who has accessed my data?

How can I prove to my auditors I am compliant?

Regulations:
- HIPAA
- PCI
- FISMA, etc.

How can I restrict how many copies are made?

How can I prevent the data being edited or printed?
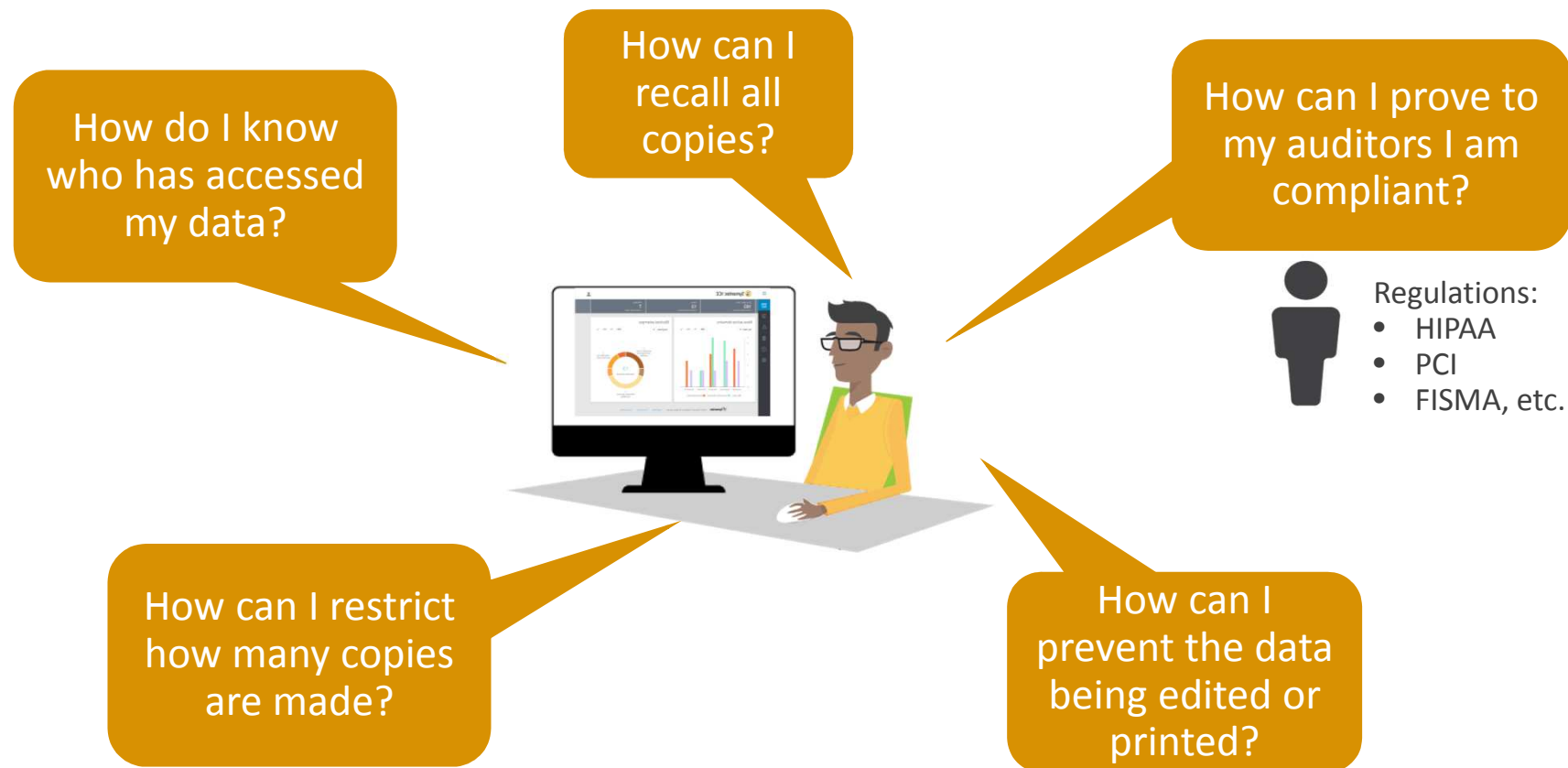
Solution: Ensure compliance using report data and access controls

- Monitor sensitive data movement within the cloud

- Show lifecycle of data wherever it resides

- Control user access even when data is outside of the organization
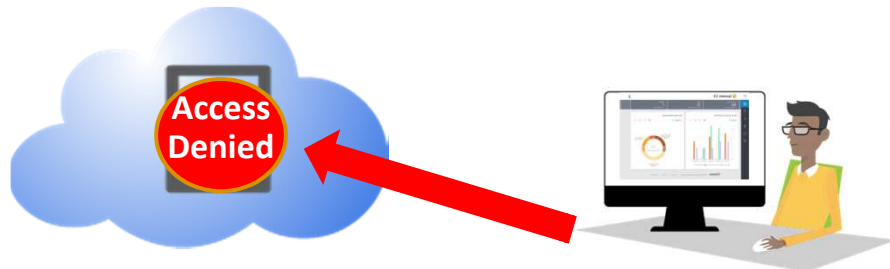
File Details

LogosRUs.docx
FILE NAME

ac97e05e-7e28-426d-828b-818ff2ddb126
FILE ID

Icedata Elastica
OWNER

7 / 34
FAILED / TOTAL ACCESS ATTEMPTS

Mar 10, 2017 07:02 PM
LAST ACCESSED

Enabled
ACCESS STATE

Mar 08, 2017 05:31 PM
REGISTRATION DATE

4
USERS

- User and file history
- user email
- filename
- time of access
- OS details

Activity   User access

Search

The following actions were performed on this file.

	Event Id	Action	User	Platform	At
	16998	Accessed	nikhilsinha@icedat...	Windows 6.1.7601 ...	Mar 10, 2017 07:02...
	16920	Accessed	nikhilsinha@icedat...	Windows 6.1.7601 ...	Mar 10, 2017 04:09...
	16919	Accessed	nikhilsinha@icedat...	Windows 6.1.7601 ...	Mar 10, 2017 04:07...

Access Denied

Symantec Information Centric Encryption

Technical Architecture

ICE architecture in context of ICS

Symantec CloudSOC

Symantec Cloud

Symantec Identity for ICE

Idp (SAML 2.0) e.g., VIP Access manager

Securlet

DLP Cloud Service Connector

OneDrive

box

ICE Admin portal

DLP Enforce

Gatelet

AWS Key Management services

Authentication

Managed devices

Unmanaged devices

ICE mobile (iOS)

Corporate Administrator

ICE Endpoint Utility

(VIP mobile app)

CloudSOC components

Symantec Cloud

Symantec
CloudSOC

Securle
t

Gatelet

OneDrive

box

DLP Cloud
Service
Connector

DLP Enforce

Managed
devices
(ICE Endpoint Utility)

Unmanaged
devices

ICE mobile
(iOS)
(VIP mobile app)

Authentication

Symantec
Identity for ICE

Idp (SAML 2.0)
VIP Access
manager

ICE Admin portal

AWS Key
Management
services

Corporate
Administrator

5

DLP components

Symantec Cloud

DLP Cloud Service Connector

DLP Enforce

Symantec CloudSOC

OneDrive

box

Symantec Identity for ICE

Idp (SAML 2.0) VIP Access manager

ICE Admin portal

AWS Key Management services

Managed devices

Unmanaged devices

ICE mobile (iOS)

ICE Endpoint Utility

VIP mobile app

Corporate Administrator

Authentication

20

ICE components

Symantec Cloud

Symantec CloudSOC

OneDrive

box

DLP Cloud Service Connector

DLP Enforce

Managed devices

Unmanaged devices

ICE mobile (iOS)

ICE Endpoint Utility

(VIP mobile app)

Idp (SAML 2.0) VIP Access manager

Symantec Identity for ICE

ICE Admin portal

AWS Key Management services

Authentication

Corporate Administrator

ICE Endpoint Utility

Symantec Cloud

Symantec
Cloud VIP

Idp (SAML 2.0)
VIP Access
manager

Symantec
Identity for ICE

DLP Cloud
Service
Connector

DLP Enforce

OneDrive

box

ICE Admin portal

AWS Key
Management
services

Authentication

Managed
devices

Unmanaged
devices

ICE mobile iOS

Symantec.
VIP

Corporate
Administrator

ICE Endpoint Utility

(VIP mobile app)

22

Context Aware Decryption

Managed Device (Employee)

- Open permissions by Default
- Favors usability of data
- Telemetry collected
- Admin can revoke rights

Pushed by IT admin to employee devices

Unmanaged Device (Partner/BYOD)

- Configurable permissions
- Favors security of data
- Content lock" features
- Telemetry on original file only

Available for download from Symantec website
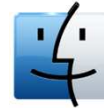
Hardware and software supported in v101

Cloud API apps
- Office365 OneDrive
- Box

ICE Endpoint Utility platform support
- Windows 7, 8, 8.1, 10
- Mac   10.10, 10.11, 10.12
- iOS 9.x, 10.x

Supported browsers
- **Admin portal** - Firefox, Chrome
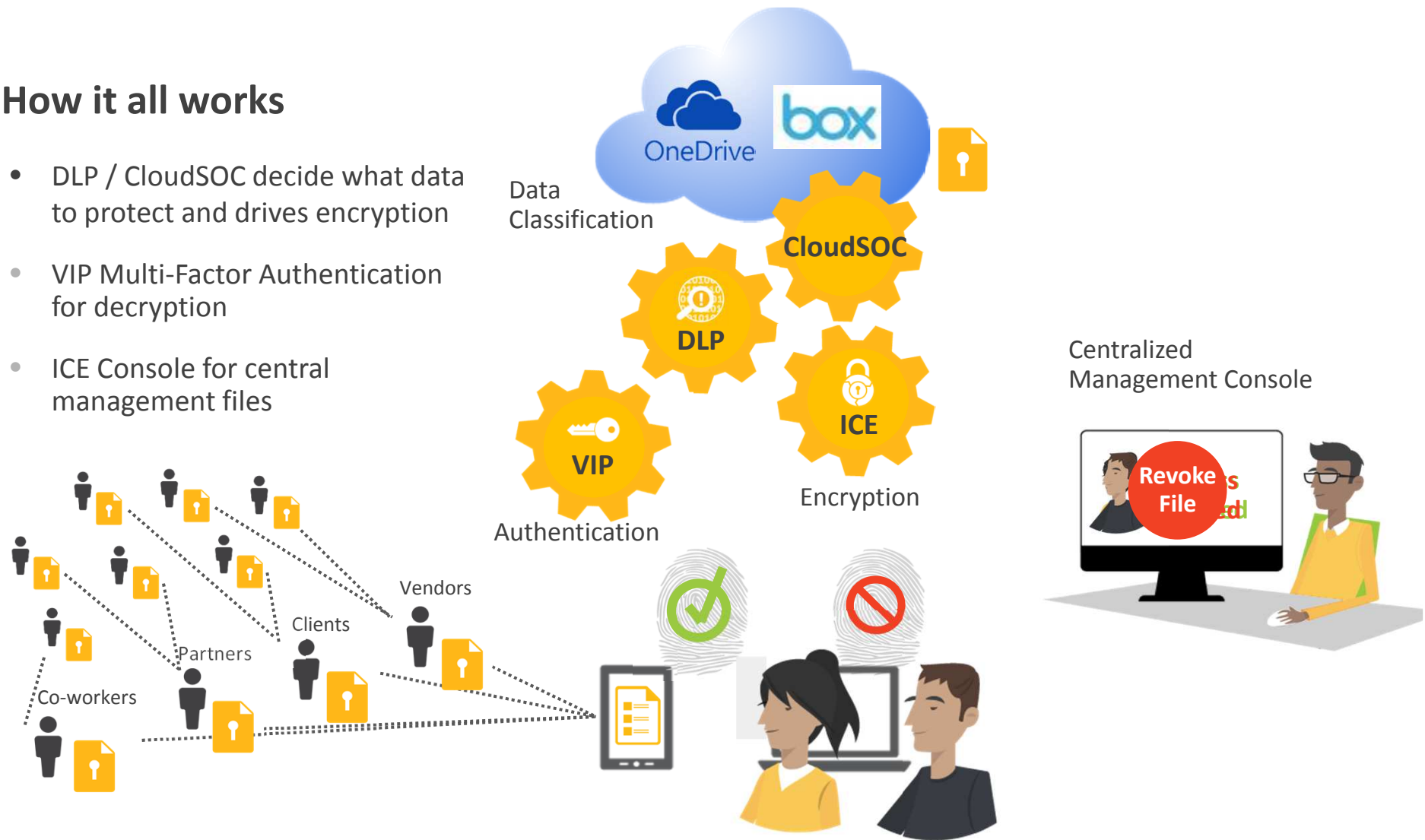- **Partner (receiving an encrypted file)** - Firefox, Chrome, IE, Safari, Edge

Symantec Information Centric Encryption

Demonstration

How it all works

- DLP / CloudSOC decide what data to protect and drives encryption

- VIP Multi-Factor Authentication for decryption

- ICE Console for central management files

Data Classification

CloudSOC

DLP

VIP

ICE

Authentication

Encryption

Centralized Management Console

Co-workers

Partners

Clients

Vendors

Revoke File

Thank you!